AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method for strong authentication achieved in a single round trip, comprising:

sending a random number to a mobile node ~~(MN)~~, wherein the random number is generated local to the ~~MN~~ mobile node, wherein the random number is generated by a base station;

generating a ~~MN~~ mobile node signature using the ~~MN~~ mobile node, wherein the ~~MN~~ mobile node signature is generated using the random number;

authenticating the ~~MN~~ mobile node to a network, wherein the network is a GPRS network; and

authenticating the network to the ~~MN~~ mobile node.

2. (Currently amended) The method of Claim 1, wherein authenticating the ~~MN~~ mobile node to the network, further comprises sending the ~~MN~~ mobile node signature to an authentication server; and verifying, by the authentication server, the mobile node signature.

3.(Canceled)

4. (Currently amended) The method of Claim 2, wherein authenticating the network to the ~~MN~~ mobile node, further comprises generating an authentication signature by the authentication server; and sending the authentication signature to the ~~MN~~ mobile node.

5. (Currently amended) The method of Claim 4, further comprising: verifying, by the ~~MN~~ mobile node, the authentication signature.

6. (Original) The method of Claim 5, wherein the authentication server is a home authentication server (AAAH).

7. (Currently amended) The method of Claim 6, wherein sending the MN signature to

the AAAH, further comprises sending the ~~MN~~ mobile node signature to a local authentication server (AAAF), wherein AAAF is located in a foreign domain and forwards the signature to the AAAH.

8. (Currently amended) The method of Claim 7, further comprising determining when the ~~MN~~ mobile node signature is not verified, and when ending the strong authentication.

9. (Original) The method of Claim 8, further comprising determining when the authentication signature is not verified, and when ending the strong authentication.

10. (Currently amended) A system for strong authentication achieved in a single round trip between a MN and a network, comprising:

a mobile node ~~(MN)~~ that is configured to generate a ~~MN~~ mobile node signature in response to a random number received from a source within a domain local to a current position relating to the ~~MN~~ mobile node and send the ~~MN~~ mobile node signature to be verified, wherein the random number is generated by a base station;

~~the~~ an authentication server located within a home domain associated with the ~~MN~~ mobile node that is configured to receive the ~~MN~~ mobile node signature, verify the ~~MN~~ mobile node signature, and in response to the verification of the ~~MN~~ mobile node signature that indicates that the ~~MN~~ mobile node is verified to the network, wherein the network is a GPRS network, return an authentication signature to the ~~MN~~ mobile node.

11. (Currently amended) The system of Claim 10, wherein the source comprises a base station, wherein the base station is within the domain local to the ~~MN~~ mobile node and is configured to generate the random number and send the random number to the ~~MN~~ mobile node.

12. (Currently amended) The system of Claim 10, further comprising: the ~~MN~~ mobile node is configured to verify the authentication signature, and if the authentication signature is verified authenticating the network to the ~~MN~~ mobile node.

13. (Currently amended) The system of Claim 11, further comprising: the ~~MN~~ mobile node is configured to verify the authentication signature, and if the authentication signature is verified authenticating the network to the ~~MN~~ mobile node.

14. (Original) The system of Claim 13, wherein the authentication server is a home authentication server (AAAH).

15. (Currently amended) The system of Claim 14, wherein sending the ~~MN~~ mobile node signature to be verified, further comprises the ~~MN~~ mobile node is configured to send the ~~MN~~ mobile node signature to a local authentication server (AAAF), and the AAAF is configured to forward the signature to the AAAH.

16. (Currently amended) The system of Claim 15, wherein the AAAH is further configured to send the authentication signature to the AAAF, wherein the AAAF is arranged to send the authentication signature to the ~~MN~~ mobile node.

17. (Currently amended) The system of Claim 16, wherein the AAAH is further configured to determine when the ~~MN~~ mobile node signature is not verified, and when, end the strong authentication.

18. (Currently amended) The system of Claim 17, wherein the ~~MN~~ mobile node is further configured to determine when the authentication signature is not verified, and when, end the strong authentication.

19. (Currently amended) A system for strong authentication between a mobile node ~~(MN)~~ and a network, comprising:

a ~~means~~ base station for generating a random number local to the ~~MN~~ mobile node;

a means for sending the random number to the mobile node

a means for generating a ~~MN~~ mobile node signature using the ~~MN~~ mobile node,

wherein the ~~MN~~ mobile node signature is generated using the random number;

a means for sending the ~~MN~~ mobile node signature to an authentication server within a GPRS network, and verifying by the authentication the ~~MN~~ mobile node signature; and in response to the verifying, generating an authentication signature and sending the authentication signature to the ~~MN~~ mobile node for verification.